UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/585,517	07/10/2006	Saar Wilf	2043.561US1	7666

49845 7590 06/01/2010

SCHWEGMAN, LUNDBERG & WOESSNER/EBAY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
MACILWINEN, JOHN MOORE JAIN	
ART UNIT	PAPER NUMBER
2442	

NOTIFICATION DATE	DELIVERY MODE
06/01/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@SLWIP.COM
request@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/585,517	WILF ET AL.	
	Examiner	Art Unit	
	John M. MacIlwinen	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39,41 and 43-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39,41 and 43-50* is/are rejected.

7)☒ Claim(s) *4* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/30/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 3/10/2010 have been fully considered.

2. Applicant's argue on page 15 that

> "Pazi merely discusses a network guard system…. In contrast, claim 1 recites 'determining... that a feature of an original source of said first information and a feature of the potential relay device are features unlikely to relate to a single device.'"

Applicant continues on page 15 arguing that

> "In Pazi, if the TTL value of the packet does not match the stored value, this indicates spoofing or packets containing bogus IP source addresses. … A TTL value of a spoofed packet is not from the same source as the stored TTL value"

In response to 2:

The Examiner agrees with Applicant's statement above from the bottom of page 15 that "A TTL value of a spoofed packet is not from the same source as the stored TTL value". If the claimed source address is detected by Pazi's disclosure as being 'bogus', then there are two devices; the legitimate device and the bogus device.

As Applicant acknowledges, Pazi shows determining that a packet is "not from the same source". This "not same … source" represents a second device. The same source/legitimate source represents a first device; thus Pazi is detecting when

communications are from two devices. Pazi's teachings of detecting two devices meets the limitations of Applicant's claim language which recites determining features "unlikely to relate to a single device". That is to say that Pazi's detection of two devices meets the limitation of detecting "unlikely … single device".

3. Applicant continues arguing on page 16 that claim 1 recites that

> "both a first information element and a second information element are received from the potential relay device"

In response to 3:

In Pazi, the claimed first information element may correspond to the claimed source address of the received data. The claimed second information element may correspond to the TTL value of the received data (Pazi, [23,30]). Said source address and said TTL value are both used to perform Pazi's detection method. Both of these are also "received from the potential relay device".

Applicant's argument thus is not persuasive.

4. Applicant continues arguing on page 16 that Pazi does not show

> "determining... that a feature of an original source of said first information and a feature of the potential relay device are features unlikely to relate to a single device".

In response to 4:

As the Examiner noted above, the Examiner agrees with Applicant's statement above from the bottom of page 15 that "A TTL value of a spoofed packet is not from the same source as the stored TTL value". If the claimed source address is detected by Pazi's disclosure as being 'bogus', then there are two devices; the legitimate device and the bogus device.

As Applicant acknowledges, Pazi shows determining that a packet is "not from the same source". This "not same … source" represents a second device. The same source/legitimate source represents a first device; thus Pazi is detecting when communications are from two devices. Pazi's teachings of detecting two devices meets the limitations of Applicant's claim language which recites determining features "unlikely to relate to a single device". That is to say that Pazi's detection of two devices meets the limitation of detecting "unlikely … single device".

5. Applicant next argues on page 16 that Mackay does not teach "

> "determining, using a relay detection system, that a feature of an original source of said first information element and a feature of the potential relay device are features unlikely to relate to a single device".

In response to 5:

Mackay was not cited to teach all of the above claim language, but rather cited for detecting relays. Mackay teaches performing said detection by analyzing TTL values

to determine the presence of a relay; specifically Mackay recites to "look for the TTL value – if it is less than the value or are expecting, then the user is behind a NAT gateway" (pg. 15, where a NAT gateway is a type of relay).

Mackay also provides further teaching regarding detecting communication unlikely to relate to a single device on page 14, describing "analysis to determine … differing machines".

Applicant's arguments, and arguments relying on those addressed above appearing on the top of page 17, thus are not persuasive.

6. Continuing on page 17, Applicant's arguments address amended claim 37. In response to said amendment, a new grounds of rejection has been made in view of Pazi2 (US 2003/0070096 A1).

Claim Objections

7. Claim 4 is objected to because of the following informalities: said claim recites the method of claim "I"; that is, [capital 'i'] rather than [numeral 'one']. Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1 – 5, 8 – 20, 32, 38, 41 and 43 – 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi (US 2003/0110274 A1) in view of Mackay (comp.os.ms-windows.networking.tcp-ip. "Can my ISP say if i'm using a proxy?" 2/16/2002. pgs. 1 - 4.).

10. Regarding claim 1, Pazi shows a method of making a determination, the method comprising:

a) receiving from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]) wherein the potential device is an original source of said second information element; and

b) determining, using a detection system implemented at least in part in hardware, that a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device (Pazi, Figs. 2,3, [7-17, 30], specifically showing determining communication bogus/hacker device and an authentic device; Pazi, [14, 23, 53, 67-68]),

said determining being indicative that the potential device is a device (Pazi, Figs. 2,3, [7-17, 30]),

Pazi does not show where the determination is: whether potential relay device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

11. Regarding claim 2, Pazi in view of Mackay further show wherein said second information element is of a type that a relay device of a class of relay devices is unlikely to relay (Mackay, pg. 2).

12. Regarding claim 3, Pazi in view of Mackay further show wherein said class of relay devices is selected from the group consisting of a SOCKS proxy, an HTTP proxy using the GET method, an HTTP proxy using the CONNECT method, an IP router and a NAT device (Mackay, pg. 2).

13. Regarding claim 4, Pazi in view of Mackay further show wherein said second information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (Mackay, pg. 2).

14. Regarding claim 5, Pazi in view of Mackay further show wherein said first information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (Mackay, pg. 2).

15. Regarding claim 8, Pazi in view of Mackay further show wherein said stage of determining comprises:

i) discovering said feature of an original source of said first information element

(Pazi, [47,55]); and

ii) discovering said feature of the potential relay device (Pazi, [47,55]).

16. Regarding claim 9, Pazi in view of Mackay further show wherein said stage of determining further comprises:

iii) comparing said feature of an original source of said first information element with said feature of the potential relay device (Pazi, [55]).

17. Regarding claim 10, Pazi in view of Mackay further show c) obtaining a parameter indicative of said feature of an original source of said first information element; and

d) obtaining a parameter indicative of said feature of the potential relay device (Pazi, [7-17] and Figs. 2, 3).

18. Regarding claim 11, Pazi in view of Mackay further show wherein said stage of determining further comprises:

iii) considering a time at which at least one of said feature of an original source of said first information element and said feature of the potential relay device, was discovered (Pazi, [44]).

19. Regarding claim 12, Pazi in view of Mackay further show c) obtaining a parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (Pazi, [44, 50-52]).

20. Regarding claim 13, Pazi in view of Mackay further show wherein said stage of determining includes analyzing said parameter indicative of a relationship between said

feature of said original source of said first information element and said feature of the potential relay device (Pazi, [44, 50-52]).

21. Regarding claim 14, Pazi in view of Mackay further show wherein said parameter is obtained from at least one of said first information element and said second information element (Pazi, [44, 50-52]).

22. Regarding claim 15, Pazi in view of Mackay further show c) sending an outgoing communication to at least one of said original source of said first information element and the potential relay device (Pazi, [16]); and

d) Receiving a third information element from said at least one of said original source of said first information element and the potential relay device (Pazi, [16-18]).

23. Regarding claim 16, Pazi in view of Mackay further show e) deriving from said third information element information related to a feature of said at least one of said original source of said first information element and the potential relay device (Pazi, [16-18, 44, 49-52]).

24. Regarding claim 17, Pazi in view of Mackay further show iii) verifying that an original source of said third information element is said original source of said first information element (Pazi, [16-18, 47]).

25. Regarding claim 18, Pazi in view of Mackay further show iii) verifying that an original source of said third information element is the potential relay device (Pazi, [54]).

26. Regarding claim 19, Pazi in view of Mackay further show wherein said third information element is selected from the group consisting of an ICMP message, an ICMP Echo Reply message, a DNS query, an HTTP request, an HTTP response, an

HTTP `Server` header, an IP address, a TCP port, a TCP Initial Sequence number, a TCP Initial Window, a WHOIS record, and a reverse DNS record (Mackay, pg. 2 and Pazi, [60-62]).

27. Regarding claim 20, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is a feature related to a configuration status (Mackay, pg. 2).

28. Regarding claim 32, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is selected from the group consisting of a sub-network, an administrator, and a location (Mackay, pgs. 1 – 2 and Pazi, [35]).

29. Regarding claim 38, Pazi shows a method of making a determination, the method comprising:

a) receiving from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]); and

b) determining, using a detection system that a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device (Pazi, Figs. 2,3, [7-17, 30], specifically showing determining communication bogus/hacker device and an authentic device; Pazi, [14, 23, 53, 67-68]),

said determining being indicative that the potential device is a device (Pazi, Figs. 2,3, [7-17, 30]),

Pazi does not show where the determination is: whether potential relay device is

a relay device and where said detection system is a relay detection system..

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system(pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

30. Regarding claim 41, Pazi shows a method of making a determination, the method comprising:

a) receiving from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]); wherein the potential device is an original source of said second information element); and

b) checking, using a detection system, whether of the potential device is different from the location of an original source of said first information element (Pazi, Figs. 2,3 and [14, 23, 53, 67-68] showing detecting a device with a different address than its claimed/spoofed address),

Pazi does not show where the determination is: whether potential relay device is a relay device and said detection system is a relay detection system.

Mackay shows making a determination using a relay detection system whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

31. Regarding claim 43, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) determining, using a detection system, whether a feature of an original source of a first information element and a feature of the potential device are features unlikely to relate to a single device (Pazi [7,15,30]),

wherein the potential device is a transmitter of said first information element and of a second information element (Pazi [7,15,30]),

wherein the potential device is an original source of said second information element (Pazi [7,15,30])

wherein a positive result of said determining is indicative that the potential device is a device (Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device and wherein said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

32. Regarding claim 44, Pazi shows a system, implemented at least in part in hardware, to determine whether a potential device is a device, the system comprising:

a) an information element receiver to receive information elements from a plurality of devices including an information source device and the potential device (Pazi [7,15,30]); and

b) a feature incompatibility analyzer, using a feature database (Pazi, [9,30]), to determine whether a feature of said information source device and a feature of the potential device are features unlikely to relate to a single device (Pazi, Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

33. Regarding claim 45, Pazi in view of Mackay further show c) a feature discovery module, for discovering at least one feature selected from the group consisting of a feature of said information source device and a feature of the potential relay device (Pazi, [55-58]).

34. Regarding claim 46, Pazi in view of Mackay further show wherein said information element receiver is further configured to receive information elements from a monitored host (Pazi, [55-58,61]).

35. Regarding claim 47, Pazi in view of Mackay further show c) an outgoing information element sender (Pazi, [61]).

36. Regarding claim 48, Pazi in view of Mackay further show c) a parameter obtainer, for obtaining at least one parameter selected from the group consisting of a parameter indicative of a feature of an information source device, a parameter indicative of a feature of the potential relay device, and a parameter indicative of whether a feature of said information source device and a feature of said potential relay device are features unlikely to relate to a single device (Pazi, Figs. 2 and 3, [52]).

37. Regarding claim 49, Pazi in view of Mackay further show c) a feature database for storing a map between pairs of features and data indicative of whether said pairs of features are incompatible features (Pazi, [47,54]).

38. Regarding claim 50, Pazi shows a computer-readable non-transitory storage medium, comprising instructions, which when executed by a computer cause the computer to:

a) receive from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]) wherein the potential device is an original source of said second information element; and

b) determine, using a detection system implemented at least in part in hardware,

that a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device (Pazi, Figs. 2,3, [7-17, 30], specifically showing determining communication bogus/hacker device and an authentic device; Pazi, [14, 23, 53, 67-68]),

wherein a positive result of said determining is indicative that the potential device is a device (Pazi, Figs. 2,3, [7-17, 30]),

Pazi does not show where the determination is: whether potential relay device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

39. Claims 6, 7 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Reed (Applying the OSI Seven Layer Network Model to Information Security. November 21, 2003).

40. Regarding claim 6, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said first and said second information elements are parts of a single communication.

Reed shows wherein said first and said second information elements are parts of a single communication (Reed, pg. 24).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

41. Regarding claim 7, Pazi in view of Mackay and Reed show wherein said first and said second information elements are sent in two different layers of a protocol stack (Reed, pg. 24).

42. Regarding claim 33, Pazi in view of Mackay show claim 32.

Pazi in view of Mackay do not show wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record.

Reed shows wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record (Reed, pgs. 23 – 24).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

43. Claims 21, 22, 23, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Nilsen (alt.comp.lang.php. "how to detect PROXY?" 12/24/2001. pgs. 1-2).

44. Regarding claim 21, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting.

Nilsen shows wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting (pg. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Nilsen more frequently be able to identify device types (Nilsen, pg. 1).

45. Regarding claim 22, Pazi in view of Mackay and Nilsen further show wherein said determining includes examining a parameter indicative of said feature related to a configuration status (Nilsen, pg. 1).

46. Regarding claim 23, Pazi in view of Mackay and Nilsen further show wherein said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` header, a protocol implementation manner, a TCP/IP stack fingerprint, an IP address, a TCP port, a TCP initial sequence number, a TCP initial window, a WHOIS record, and a reverse DNS record (Mackay, pg. 2)

47. Regarding claim 34, Pazi shows a method of determining whether a potential device is a relay device, the method comprising:

a) receiving from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]) wherein the potential device is an original source of said second information element

b) analyzing a configuration status of an original source of at least one of said first and said second information elements (Pazi, [7-17])

c) determining, using a detection system, whether a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device Pazi, Figs. 2,3, [7-17, 30], specifically showing determining communication bogus/hacker device and an authentic device; Pazi, [14, 23, 53, 67-68]),

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting.

Nilsen shows said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting (pg. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Nilsen more frequently be able to identify device types (Nilsen, pg. 1).

48. Claims 24 – 31, 35,36 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Daude (US 6,892,235 B1).

49. Regarding claim 24, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not explicitly show wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance.

Daude shows wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance (col. 7 lines 25 - 34, Figs. 5 – 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (Daude, col. 7 lines 25 - 34)

50. Regarding claim 25, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a measured communication performance, a measured relative communication performance, and an estimated communication performance (Daude, Figs. 5 – 7).

51. Regarding claim 26, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a

latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (Daude, col. 8 lines 36 – 40).

52. Regarding claim 27, Pazi in view of Mackay and Daude further show wherein said determining includes examining a parameter indicative of said feature related to communication performance (Pazi, [34]).

53. Regarding claim 28, Pazi in view of Mackay and Daude further show wherein said parameter is selected from the group consisting of time of receipt of an information element, time of sending of an information element, a round trip time, a round trip time gap, an IP address, a Whois record, a reverse DNS record, and a rate of acknowledged information (Daude, col. 8 lines 36 – 40).

54. Regarding claim 29, Pazi in view of Mackay and Daude further show wherein a higher round trip time gap is indicative of a higher likelihood that a relay device is being used for malicious purposes (Daude, col. 8 lines 60 – 65).

55. Regarding claim 30, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is estimated from information about at least one of said original source of said first communication and the potential relay device (Daude, Abstract).

56. Regarding claim 31, Pazi in view of Mackay and Daude further show wherein said information about at least one of said original source of said first communication and the potential relay device is selected from the group consisting of a location of a

device, a reverse DNS record of a device's IP address, and an administrator of a device (Daude, col. 11 lines 48 – 60).

57. Regarding claim 35, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) receiving from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]) wherein the potential device is an original source of said second information element

analyzing, using a detection system, a feature of an original source of at least one of said first and said second information elements (Pazi, [7,15,30])

determining, using a detection system, whether a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device (Pazi, Figs. 2,3, [7-17, 30], specifically showing determining communication bogus/hacker device and an authentic device; Pazi, [14, 23, 53, 67-68]),

Pazi does not show where the determination is: whether potential relay device is a relay device and where the detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device and where the detection system is a relay detection system (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show b) analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements.

Daude shows b) analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements (col. 7 lines 25 – 34, Figs. 5 – 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (Daude, col. 7 lines 25 – 34).

58. Regarding claim 36, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (Daude, col. 8 lines 36 – 40).

59. Regarding claim 39, Pazi shows method of determining whether a potential device is a device, the method comprising:

a) receiving from the potential device a first information element (e.g., a claimed source address, Pazi [7,15,30]) and a second information element (e.g., a TTL value, Pazi [7,15,30]) wherein the potential device is an original source of said second

information element

b) checking, using a detection system, whether an element related to the potential device is significantly different than an element related to an original source of said first information element (Pazi, [7,15,30]).

Pazi does not show where the determination is: whether potential relay device is a relay device and where the detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device and where the detection system is a relay detection system (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show checking round-trip times.

Daude shows checking round-trip times (Figs. 1, 4, 6 and col. 8 lines 25 – 65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (Daude, col. 7 lines 24 - 35).

60. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi et al. (US 2003/0070096 A1), hereafter Pazi2 (where Pazi, US 2003/0110274 is incorporated by reference into Pazi2 in Pazi2, [1]) in view of Mackay.

61. Regarding claim 37, Pazi 2 shows a method of determining whether a potential device is a device, the method comprising:

a) sending a message to an information source device, triggering said information source device to send a DNS request to a DNS server (Pazi2, Fig. 2 items 42 and 44)

b) monitoring said DNS request from said information source device to said DNS server (Pazi2, item 46)

c) determining, using a detection system, from said DNS request whether said potential device is a device (Pazi2, items 48 – 52 and [18-19]).

Pazi2 does not show where the determination is: whether potential relay device is a relay device and where the detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device and where the detection system is a relay detection system (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi2 with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Philip Lee, can be reached at (571) 272 - 3967. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John MacIlwinen

(571) 272 - 9686

/Philip C Lee/
Acting Supervisory Patent Examiner, Art Unit 2442